What is claimed is

1. A traceback connection apparatus comprising:

a packet blocking unit, which if a system attack sensing signal is received, blocks an attack packet transmitted to a system and a first response packet output from the system in response to the attack packet;

a response packet generation unit, which generates a second response packet into which a watermark is inserted, in response to the attack packet, and transmits the second response packet to a system corresponding to the source address of the attack packet; and

a path traceback unit, which receives a detection packet containing transmission path information of the second response packet from a system existing on a transmission path of the second response packet, and based on the received detection packet, traces back the transmission path of the second response packet and identifies the location of the attacker system.

2. The apparatus of claim 1, further comprising:

an attack detection unit, which if a system attack by an external attacker is sensed, outputs an attack sensing signal containing the IP addresses of the source and destination of the attack path and the port number.

3. The apparatus of claim 2, wherein the attack detection unit senses a system attack by the external attacker by investigating log files of the system, log files of a network, and whether or not a predetermined system file has been changed, and based on the log file of the system, identifies the IP address of the source and port number of the attack packet.

4. The apparatus of claim 2, wherein the packet blocking unit comprises:

a signal reception unit, which receives the attack sensing signal;

a packet identifying unit, which identifies the attack packet and the first response packet based on the IP addresses and the port number; and

a blocking unit, which blocks the attack packet and the first response packet.

5. The apparatus of claim 1, further comprising:

a watermark detection unit, which if a packet containing a watermark from an external network is received, transmits a detection packet containing the path information of the received packet to a system of the external network which inserted the watermark.

6. The apparatus of claim 5, wherein the watermark detection unit comprises:

a detection unit, which detects a watermark contained in a packet received from the outside;

a detection packet generation unit, which if a watermark is detected, generates a detection packet containing the IP addresses of the source and destination and port number of the received packet; and

a packet transmission unit, which transmits the generated detection packet to a system that first inserted the watermark to the packet.

7. The apparatus of claim 1, wherein the path traceback unit traces back the location of an attacker system based on the IP addresses of the source and destination and port number contained in the one or more received detection packets.

8. A traceback connection method comprising:

blocking an attack packet transmitted to the system and a first response packet output from a system in response to the attack packet, if a system invasion sensing signal is received;

generating a second response packet into which a watermark is inserted, in response to the attack packet, and transmitting the second response packet to a system corresponding to the source address of the attack packet; and

receiving a detection packet containing transmission path information of the second response packet from a system existing on a transmission path of

the second response packet, and based on the received detection packet, tracing back the transmission path of the second response packet and identifying the location of the attacker system.

9. The method of claim 8, further comprising:

outputting an attack sensing signal containing the IP addresses of the source and destination of the attack path and the port number before the blocking, if a system attack by an external attacker is sensed.

10. The method of claim 9, wherein the blocking comprises:

receiving the attack sensing signal;

identifying the attack packet and the first response packet based on the IP addresses and the port number; and

blocking the attack packet and the first response packet.

11. The method of claim 8, further comprising:

transmitting a predetermined detection packet to a system of the external network which inserted the watermark, if a packet containing a watermark from an external network is received.

12. The method of claim 11, wherein transmitting a detection packet comprises:

detecting a watermark contained in a receive packet;

if the watermark is detected, generating a detection packet containing the IP addresses of the source and destination and port number of the received packet; and

transmitting the generated detection packet to a system that first inserted the watermark to the packet.

13. The method of claim 8, wherein the tracking back the transmission path comprises:

tracking back the location of an attacker system based on the IP addresses of the source and destination and port number contained in the one or more received detection packets.

14. A computer readable medium having embodied thereon a computer program for executing a traceback connection method comprising:

blocking an attack packet transmitted to the system and a first response packet output from the system as a response to the attack packet, if a system invasion sensing signal is received;

generating a second response packet into which a watermark is inserted, in response to the attack packet, and transmitting the second response packet to a system corresponding to the source address of the attack packet; and

receiving a detection packet containing transmission path information of the second response packet from a system existing on a transmission path of the second response packet, and based on the received detection packet, tracing back the transmission path of the second response packet and identifying the location of the attacker system.